ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-13-011-02— SPECVIEW DIRECTORY TRAVERSAL

January 11, 2013

OVERVIEW

This advisory is a follow up to the original alert titled ICS-ALERT-12-214-01—SpecView Directory Traversal that was published August 01, 2012, on the ICS-CERT Web. This advisory provides mitigation details for a vulnerability, which impacts SpecView products.

Independent researcher Luigi Auriemma identified a directory traversal vulnerability with proof-of-concept (PoC) exploit code affecting SpecView, a supervisory control and data acquisition/human-machine interface (SCADA/HMI) product. Successful exploitation could result in data leakage and file manipulation. This report was released without coordination with either the vendor or ICS-CERT.

This vulnerability could be exploited remotely. Exploits that target this vulnerability are publicly available.

SpecView has released a new build that addresses this vulnerability. Luigi Auriemma has verified the new build fixes the vulnerability.

AFFECTED PRODUCTS

The following SpecView versions are affected:

- SpecView 2.5 Build 853 and earlier.

IMPACT

Successful exploitation could result in data leakage and file manipulation.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

BACKGROUND

SpecView is a US-based company that maintains offices in the United States and United Kingdom.

The affected product, SpecView, is HMI software for SCADA equipment. SpecView is used worldwide in various industries, primarily in critical manufacturing.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

DIRECTORY TRAVERSAL[a]

By sending specially crafted packets to the SpecView webserver on Port 80/TCP, an attacker can cause a path traversal.

CVE-2012-5972[b] has been assigned to this vulnerability. A CVSS v2 base score of 2.6 has been assigned; the CVSS vector string is (AV:N/AC:H/Au:N/C:P/I:N/A:N).[c]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

Exploits that target this vulnerability are publicly available.

DIFFICULTY

An attacker with a high skill would be able to exploit this vulnerability.

a. Path Traversal, http://cwe.mitre.org/data/definitions/23.html, CWE-23: Relative Path Traversal, Web site last accessed January 11, 2013.

b. NVD, http://web.nvd nist.gov/view/vuln/detail?vulnId=CVE-2012-5972, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

c. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:H/Au:N/C:P/I:N/A:N), Web site last visited January 11, 2013.

MITIGATION

SpecView recommends users download and install the update[d] from their web site which mitigates the vulnerability.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT also provides a section for control systems security recommended practices on the US-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[e] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01A—Targeted Cyber Intrusion Detection and Mitigation Strategies,[f] that is available for download from the ICS-CERT Web page (www.ics-cert.org).

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585

---

d. SpecView Update, http://www.specview.com/html/downloads html, Web site last accessed January 11, 2013.

e. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices html, Web site last accessed January 11, 2013.

f. Targeted Cyber Intrusion Detection and Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed January 11, 2013.

For industrial control systems security information and incident reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.